Understanding Network Communication and Data Packets

* Data Packets and Their Role:
  + A data packet is the basic unit of information transferred across a network.
  + Packets contain details such as the destination IP address, source IP address, and the content being sent.
  + The structure of a packet includes:
    - A header (with destination and source addresses).
    - A body (containing the actual message).
    - A footer (indicating the end of the packet).
* Network Performance Metrics:
  + Bandwidth: Measures the amount of data a device can receive per second, calculated by dividing the data volume by time.
  + Speed: Refers to the rate at which packets are sent or received.
  + Abnormalities in bandwidth or speed may signal a network attack.
* Security Considerations:
  + Packet Sniffing: The practice of capturing and analyzing data packets to monitor network activity.
  + Monitoring packet movement helps ensure efficient communication and identify potential vulnerabilities or attacks.

Understanding the TCP/IP Model and Network Communication

* What is TCP/IP?
  + TCP (Transmission Control Protocol) establishes connections and ensures data is delivered correctly between devices on a network.
  + IP (Internet Protocol) handles the routing and addressing of data packets across the network, assigning unique IP addresses to devices.
* Ports in Network Communication:
  + A port is a software-based location on a device that organizes the sending and receiving of data packets.
  + Ports help prioritize network traffic and segment data based on the type of service (e.g., email, secure browsing, file transfers).
* Examples of Common Port Numbers:
  + Port 25: Used for email communication.
  + Port 443: Used for secure internet communication (HTTPS).
  + Port 20: Used for large file transfers (FTP).

The TCP/IP Model and Its Four Layers

1. Network Access Layer:
   * Focuses on the creation of data packets and their transmission over physical hardware like cables and switches.
   * Ensures data reaches its destination via physical connections.
2. Internet Layer:
   * Adds IP addresses to data packets for identifying sender and receiver locations.
   * Manages how networks connect to each other, including whether data stays on a LAN or is sent to external networks like the internet.
3. Transport Layer:
   * Manages data flow across the network, using protocols to control and regulate communication.
   * Includes error control, ensuring smooth data transmission.
4. Application Layer:
   * Determines how data packets interact with receiving devices, supporting functions like file transfers and email services.

Learn more about the TCP/IP model

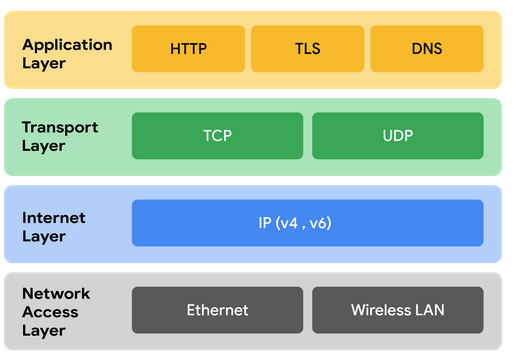
In this reading, you will build on what you have learned about the Transmission Control Protocol/Internet Protocol (TCP/IP) model, consider the differences between the Open Systems Interconnection (OSI) model and TCP/IP model, and learn how they’re related. Then, you’ll review each layer of the TCP/IP model and go over common protocols used in each layer.

As a security professional, it's important that you understand the TCP/IP model because it describes the functions of various network protocols. The TCP/IP model is based on the TCP/IP protocols suite that includes all network protocols that support the main TCP/IP protocol. To reiterate from previous lessons, a network protocol, also known as an internet protocol, is a set of standards used for routing and addressing data packets as they travel between devices on a network. In this reading, you will learn which network protocols operate on which communication layers of the TCP/IP model. The two most common models available are the TCP/IP and the OSI model. These models are a representative guideline of how hosts communicate across a network. The examples provided in this course will follow the TCP/IP model.

The TCP/IP model

The TCP/IP model is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze which layers were impacted by an attack based on what processes were involved in an incident.



Network access layer

The network access layer, sometimes called the data link layer, deals with the creation of data packets and their transmission across a network. This layer corresponds to the physical hardware involved in network transmission. Hubs, modems, cables, and wiring are all considered part of this layer. The address resolution protocol (ARP) is part of the network access layer. Since MAC addresses are used to identify hosts on the same physical network, ARP is needed to map IP addresses to MAC addresses for local network communication.

Internet layer

The internet layer, sometimes referred to as the network layer, is responsible for ensuring the delivery to the destination host, which potentially resides on a different network. It ensures IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host. Here are some of the common protocols that operate at the internet layer:

* Internet Protocol (IP). IP sends the data packets to the correct destination and relies on the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. TCP in particular retransmits any data that is lost or corrupt.
* Internet Control Message Protocol (ICMP). The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers.

Transport layer

The transport layer is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network. TCP and UDP are the two transport protocols that occur at this layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet.

User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming.

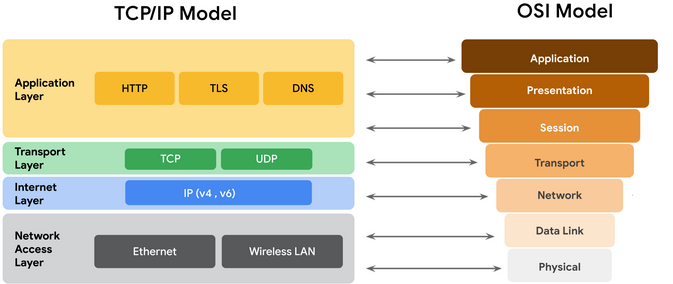
Application layer

The application layer in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Protocols in the application layer determine how the data packets will interact with receiving devices. Some common protocols used on this layer are:

* Hypertext transfer protocol (HTTP)
* Simple mail transfer protocol (SMTP)
* Secure shell (SSH)
* File transfer protocol (FTP)
* Domain name system (DNS)

Application layer protocols rely on underlying layers to transfer the data across the network.

TCP/IP model versus OSI model



The OSI visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

The TCP/IP model combines multiple layers of the OSI model. There are many similarities between the two models. Both models define standards for networking and divide the network communication process into different layers. The TCP/IP model is a simplified version of the OSI model.

Key takeaways

Both the TCP/IP and OSI models are conceptual models that help network professionals visualize network processes and protocols in regards to data transmission between two or more systems. The TCP/IP model contains four layers, and the OSI model contains seven layers.

# The OSI model

So far in this section of the course, you learned about the components of a network, network devices, and how communication occurs across a network. You also studied the TCP/IP model to understand how network communication is organized across different layers of the internet.

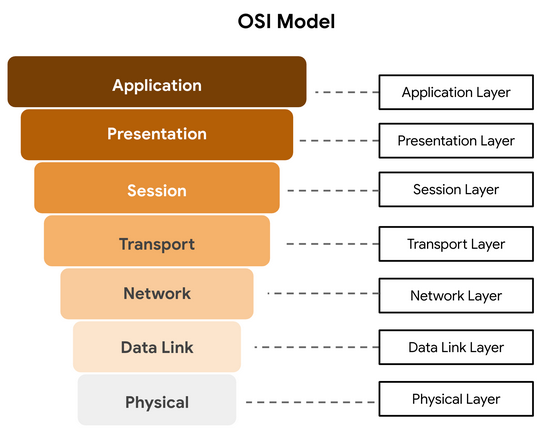
All communication on a network is organized using network protocols. Previously, you learned about the Transmission Control Protocol (TCP), which establishes connections between two devices, and the Internet Protocol (IP), which is used for routing and addressing data packets as they travel between devices on a network. These protocols are used on specific internet layers in the TCP/IP model. The 4-layer TCP/IP model is a condensed form of the OSI (open Systems Interconnection) model, which is made up of 7 layers. The OSI model will provide a more in depth understanding of the processes that occur at each layer. We will work backwards from layer seven to layer one, going from the processes that involve direct user interaction with the network to those that involve the physical connection to the internet via network components like cables and switches. This reading will also review the main differences between the TCP/IP and OSI models.

## The TCP/IP model vs. the OSI model

The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When analyzing network events, security professionals can determine what layer or layers an attack occurred in based on what processes were involved in the incident.

The **OSI model** is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.



Some organizations rely heavily on the TCP/IP model, while others prefer to use the OSI model. As a security analyst, it’s important to be familiar with both models. Both the TCP/IP and OSI models are useful for understanding how networks work.

## Layer 7: Application layer

The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of the application layer—user connection to the internet via applications and requests.

An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website.

## Layer 6: Presentation layer

Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format.

Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS.

## Layer 5: Session layer

A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols keep the session open while data is being transferred and terminate the session once the transmission is complete.

The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4).

## Layer 4: Transport layer

The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport. Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols.

## Layer 3: Network layer

The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network.

## Layer 2: Data link layer

The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices.

Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer.

## Layer 1: Physical layer

As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model.

## Key takeaways

Both the TCP/IP and OSI models are conceptual models that help network professionals design network processes and protocols with regards to data transmission between two or more systems. The OSI model contains seven communication layers. Network and security professionals use the OSI model to communicate with each other about potential sources of problems or security threats when they occur.  Network engineers and network security analysts use the TCP/IP and OSI models to conceptualize network processes and communicate the location of disruptions or threats.